Substitute for HOUSE BILL NO. 2560

By Committee on Government, Technology and Security

AN ACT concerning information systems and communications; creating the Kansas cybersecurity act; establishing the Kansas information security office; establishing the cybersecurity state fund.

Be it enacted by the Legislature of the State of Kansas:

Section 1. Sections 1 through 15, and amendments thereto, shall be known and may be cited as the Kansas cybersecurity act.

Sec. 2. As used in sections 1 through 15, and amendments thereto:

(a) "Act" means the Kansas cybersecurity act.

(b) "Breach" or "breach of security" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the executive branch agency does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

(c) "CISO" means the executive branch chief information security officer.

(d) "Cybersecurity" is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

(e) "Cybersecurity positions" do not include information technology positions within governmental entities

(f) "Data in electronic form" means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(g) "Executive branch" means any governmental entity in the executive branch of the state of Kansas, but does not include elected office agencies, the Kansas public employees

retirement system, regents' institutions, or the board of regents.

(h) "Governmental entity" means any department, division, bureau, commission, regional planning agency, board, district, authority, agency or other instrumentality of the executive branch that acquires, maintains, stores or uses data in electronic form containing personal information, but does not include the Kansas public employees retirement system.

(i) "KISO" means the Kansas information security office.

(i) "Municipality" shall have the meaning ascribed to it in K.S.A. 75-6102, and amendments thereto.

(j) (1) "Personal information" means:

(A) An individual's first name or first initial and last name, in combination with at least one of the following data elements for that individual:

(i) Social security number;

(ii) driver's license or identification card number, passport number, military identification number or other similar number issued on a government document used to verify identity;

(iii) financial account number or credit or debit card number, in combination with any security code, access code or password that is necessary to permit access to an individual's financial account;

(iv) any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a health care professional; or

(v) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or

(B) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(2) "Personal information" does not include information:

(A) About an individual that has been made publicly available by a federal agency, state agency or municipality; or

(B) that is encrypted, secured or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

(k) "State network resources" means any transmission, emission or reception of data of any kind containing communications of any nature, by wire, radio, optical or other electromagnetic means, including all facilities, equipment, supplies and services for such transmission, emission or reception that is owned, operated or managed by the state of Kansas.

Sec. 3. (a) There is hereby established the position of executive branch chief information security officer. The CISO shall be in the unclassified service under the Kansas civil service act, shall be appointed by the governor and shall receive compensation in an amount fixed by the governor.

(b) The CISO shall have a current, valid federal security clearance at the appropriate level or be able to obtain such clearance within six months of appointment.

(c) The CISO shall:

(1) Report to the executive branch chief information technology officer;

(2) serve as the state's CISO;

(3) serve as the executive branch chief cybersecurity strategist and authority on

policies, compliance, procedures, guidance and technologies impacting executive branch cybersecurity programs;

(4) ensure cybersecurity training programs are provided for the executive branch;

(5) ensure technology resources assigned or provided to governmental entities are in compliance with applicable laws and rules and regulations and the national institute of standards technology cybersecurity framework or equivalent industry standard;

(6) ensure personnel resources assigned or provided to governmental entities report to the entity's appropriate executive leadership;

(7) coordinate cybersecurity efforts among governmental entities at the state and municipality level and private vendors;

(8) provide an annual report on the economic impact of cybersecurity insurance as a mitigation measure for datea breach or unauthorized disclosure of personal information to the house government, technology and security committee, or its successor committee.

(9) have authority to:

(A) Oversee and approve executive branch cybersecurity plans for information technology projects;

(B) halt executive branch information technology projects or information systems that are not compliant with approved cybersecurity plans;

(C) conduct ad hoc security assessments of executive branch information systems and internal information technology operating environments;

(D) suspend public access to executive branch information resources when compromise of personal information or computer resources have occurred or is likely to occur as the result of

an identified high-risk vulnerability or threat; and

(E) hire, promote, suspend, demote, discipline and dismiss all executive branch cybersecurity positions; and

(10) perform such other functions and duties as provided by law and as directed by the executive chief information technology officer.

Sec. 4. (a) There is hereby established the Kansas information security office. The Kansas information security office shall be administered by the CISO and be staffed appropriately to effect the provisions of the Kansas cybersecurity act.

(b) For the purpose of preparing the governor's budget report and related legislative measures submitted to the legislature, the Kansas information security office, established in this section, shall be considered a separate state agency and shall be titled for such purpose as the "Kansas information security office." The budget estimates and requests of such office shall be presented as from a state agency separate from the department of administration, and such separation shall be maintained in the budget documents and reports prepared by the director of the budget and the governor, or either of them, including all related legislative reports and measures submitted to the legislature.

(c) Under direction of the CISO, the KISO shall:

(1) Administer the Kansas cybersecurity act;

(2) assist the executive branch in developing, implementing and monitoring strategic and comprehensive information security risk-management programs;

(3) provide the executive branch strategic risk guidance for information technology projects, including the evaluation and recommendation of technical controls;

(4) facilitate the executive branch information security governance, including the formation of an information security steering committee or advisory board, which shall include representation from cabinet and non-cabinet agencies of the executive branch;

(5) create and manage a unified and flexible control framework to integrate and normalize requirements resulting from global laws, standards and regulations;

(6) ensure that security programs and technology solutions offered by vendors to the state are in compliance with relevant laws, rules and regulations and policies;

(7) provide the executive branch contract provisions with information security language for compliance requirements to expedite review of contracts for security programs and technology solutions;

(8) facilitate a metrics, logging and reporting framework to measure the efficiency and effectiveness of state information security programs;

(9) coordinate the use of external resources involved in information security programs, including, but not limited to, interviewing and negotiating contracts and fee*s;*

(10) liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure a strong security posture;

(11) assist in the development of effective disaster recovery policies and standards;

(12) assist in the development of implementation plans and procedures to ensure that business-critical services are recovered in a cybersecurity event;

(13) coordinate information technology security interests among governmental entities at the municipality and state levels; and

(14) perform such other functions and duties as provided by law and as directed by the

CISO.

Sec. 5. (a) The executive director or agency head of any governmental entity connecting to state network resources shall:

(1) Be solely responsible for security of all data and information technology resources under such entity's purview, irrespective of the location of the data or resources. Locations of data may include: (A) Entity sites; (B) entity real property; (C) infrastructure in state data centers; (D) third-party locations; and (E) in transit between locations;

(2) ensure that an entity-wide information security program is in place;

(3) designate an information security officer to administer the entity's information security program that reports directly to executive leadership;

(4) participate in CISO-sponsored statewide cybersecurity program initiatives and services;

(5) implement policies and standards to ensure that all the entity's data and information technology resources are maintained in compliance with applicable state and federal laws and rules and regulations and the national institute of standards technology cybersecurity framework or equivalent industry standard;

(6) implement appropriate cost-effective safeguards to reduce, eliminate or recover from identified threats to data and information technology resources;

(7) include all appropriate cybersecurity requirements in the entity's request for proposal specifications for procuring data and information technology systems and services;

(8) (A) submit a cybersecurity assessment report to the CISO by October 16 of each even-numbered year, including an executive summary of the findings, that assesses the extent to

which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or the data processing of the entity or of a contractor of the entity is vulnerable to unauthorized access or harm, including the extent to which the entity's or contractor's electronically stored information is vulnerable to alteration, damage, erasure or inappropriate use;

(B) ensure that the entity conducts annual internal assessments of its security program. Internal assessment results shall be considered confidential and shall not be subject to discovery by or release to any person or entity outside of the KISO or CISO. This provision regarding confidentiality shall expire on July 1, 2023, unless the legislature reviews and reenacts such provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2023; and

(C) prepare or have prepared a summary of the cybersecurity assessment report required in subparagraph (A), excluding information that might put the data or information resources of the entity or its contractors at risk. Such report shall be made available to the public upon request;

(9) participate in annual entity leadership training to ensure understanding of: (A) The information and information systems that support the operations and assets of the entity; (B) the potential impact of common types of cyberattacks and data breaches on the entity's operations and assets; (C) how cyberattacks and data breaches on the entity's operations and assets could impact the operations and assets of other governmental entities on the state enterprise network; (D) how cyberattacks and data breaches occur; (E) steps to be undertaken by the executive director or agency head and entity employees to protect their information and information systems; and (F) the annual reporting requirements required of the executive director or agency

head; and

(10) ensure that if an entity owns, licenses or maintains computerized data that includes personal information, confidential information or information, the disclosure of which is regulated by law, shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(A) Comply with the notification requirements set out in K.S.A. 2017 Supp. 50-7a01 et seq., and amendments thereto, and applicable federal law and rules and regulations, to the same extent as a person who conducts business in this state; and

(B) not later than 48 hours after the discovery of the breach, suspected breach or unauthorized exposure, notify: (i) The CISO; and (ii) if the breach, suspected breach or unauthorized exposure involves election data, the secretary of state.

Sec. 6. (a) All governmental entities or private entities connecting to state network resources, shall demonstrate cybersecurity effectiveness by validating both technical and non-technical cybersecurity controls that constitute information security programs. Validation reports of these controls shall be provided to the CISO biennially. Reports provided to the CISO shall:

(1) Demonstrate the ability to meet applicable cybersecurity state and federal laws, rules and regulations, and policies through security assessments;

(2) include an itemized list of all cybersecurity expenditures through accounts payable reports;

(3) include the positions, qualifications and duties of all cybersecurity staff through personnel records or equivalent information when third parties are used; and

(4) demonstrate the entity's ability to secure the information of Kansas citizens and

businesses.

(b) (1) Cybersecurity plans shall be reviewed and approved by entity heads annually.

(2) The CISO shall review an entity's validation reports and cybersecurity plans to make recommendations to respective executive directors or agency heads and the governor.

(c) An entity shall not be disconnected from state network resources unless the CISO determines the existence of an imminent, critical threat. If such a threat is identified, the CISO may temporarily disconnect an entity from the state network until the identified threat is removed.

Sec. 7. (a) Governmental entities shall adopt and implement a policy to protect the privacy of individuals or businesses by preserving the confidentiality of information processed by their websites or applications. Each entity shall submit such policy to the CISO for review and recommendation.

(b) Before deploying an internet website or mobile application that processes confidential or personal information:

(1) The developer of the website or application shall submit to the governmental entity's information security officer the information required under policies adopted by the entity. The entity's policies shall require the developer to submit for approval a detailed security plan that addresses at a minimum: (A) The architecture of the website or application; (B) the authentication mechanism for the website or application; (C) logging strategy that addresses specific data elements to be recorded; (D) security of data in transit; (E) security of data at rest; and (F) the administrator level access to data included in the website or application; and

(2) the governmental entities shall subject the website or application to a vulnerability

and penetration test conducted internally or by an independent third party.

Sec. 8. (a) An executive director or agency head, with input from the CISO, may require employees or contractors of governmental entities whose duties include collection, maintenance or access to personal information to be fingerprinted and to submit to a state and national criminal history record check at least every five years.

(b) The fingerprints shall be used to identify the employee and to determine whether the employee or other such person has a record of criminal history in this state or another jurisdiction. The executive director or entity head shall submit the fingerprints to the Kansas bureau of investigation and the federal bureau of investigation for a state and national criminal history record check. The executive director or agency head may use the information obtained from fingerprinting and the criminal history record check for purposes of verifying the identity of the employee or other such person and in the official determination of the qualifications and fitness of the employee or other such person to work in the position with access to personal information.

(c) Local and state law enforcement officers and agencies shall assist the executive director or entity head in the taking and processing of fingerprints of employees or other such persons. Local law enforcement officers and agencies may charge a fee as reimbursement for expenses incurred in taking and processing fingerprints under this section, to be paid by the governmental entity employing or contracting the individual required to submit to fingerprinting and a criminal history record check.

Sec. 9. Information collected to effectuate this act shall be considered confidential by the governmental entity and KISO unless all data elements or information that specifically

identifies a target, vulnerability or weakness that would place the organization at risk has been redacted, including: (a) System information logs; (b) vulnerability reports; (c) risk assessment reports; (d) system security plans; (e) detailed system design plans; (f) network or system diagrams; and (g) audit reports. The provisions of this section shall expire on July 1, 2023, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2023.

Sec. 10. (a) There is hereby established in the state treasury the cybersecurity state fund, which shall be administered by the CISO. All expenditures from the cybersecurity state fund shall be made in accordance with appropriation acts upon warrants of the director of accounts and reports issued pursuant to vouchers approved by the CISO or the designee of the CISO. All moneys received pursuant to the provisions of the Kansas cybersecurity act shall be deposited in the state treasury in accordance with the provisions of K.S.A. 75-4215, and amendments thereto, and shall be credited to the cybersecurity state fund.

(b) All moneys received by the cybersecurity state fund shall be used only for necessary and reasonable costs incurred or to be incurred by the KISO for: (1) Implementation and delivery of cybersecurity services; (2) purchase, maintenance and license fees for cybersecurity and supporting equipment and upgrades; (3) purchase, maintenance and license fees for cybersecurity and supporting software and upgrades; (4) training of personnel; (5) installation, service establishment, start-up charges and monthly recurring charges billed by service suppliers; (6) capital improvements and equipment or other physical enhancements to the cybersecurity program; (7) projects involving the development and implementation of cybersecurity services; (8) cybersecurity consolidation or cost-sharing projects; (9) delivery of cybersecurity services;

(10) maintenance of adequate staffing, facilities and support services of the KISO; (11) projects involving the development and implementation of cybersecurity services for municipalities; (12) municipality consolidation or cost-sharing cybersecurity projects; (13) promotion of cybersecurity education; (14) development and implementation of a cybersecurity scholarship program; and (15) cybersecurity insurance.

Sec. 11. Appropriations may be made for capital outlay and other expenses to carry out the purposes of the KISO for the same period as is authorized by K.S.A. 46-155, and amendments thereto, for capital improvements. The CISO may enter into multiple-year lease or acquisition contracts, subject to state leasing and purchasing laws not in conflict with the foregoing authorization and so long as such contracts do not extend beyond the appropriation periods, limitations and restrictions therefor.

Sec. 12. (a) The CISO may adopt rules and regulations providing for the administration of this act, including:

(1) Establishment of rates and charges for services performed by the KISO for any governmental entity. Such rates and charges shall be maintained by a cost system in accordance with generally accepted accounting principles. In determining cost rates for billing governmental entities, overhead expenses shall include, but not be limited to, light, heat, power, insurance, labor and depreciation. Billings shall include direct and indirect costs and shall be based on the foregoing cost accounting practices;

(2) a fee structure for non-executive branch governmental entities connecting to the state network based on how many employees in each entity are connected to state network resources;

(3) determination of priorities for services performed by the KISO, including authority to decline new projects under specified conditions, with project determinations made within 30 days after receipt of a completed request for approval or review, when practicable;

(4) the manner of performance of any power or duty of the KISO;

(5) the execution of any business of such office and its relations to and business with other state agencies;

(6) appeals from the final decisions or final actions of the CISO; and

(7) policies for identification of information security vulnerabilities within entities, development of procedures with entities to address identified vulnerabilities and the assistance provided to entities to implement procedures to address vulnerabilities;

(b) (1) To establish a base rate for effectuating the provisions of this act, there is hereby imposed a basic cybersecurity service rate for the executive branch:

(A) For fiscal year 2019, this rate shall not exceed $350 per employee connecting to the state network per year;

(B) for fiscal year 2020, this rate shall not exceed $360 per employee connecting to the state network per year; and

(C) for fiscal year 2021, this rate shall not exceed $400 per employee connecting to the state network per year.

(2) Network connection rates paid by non-executive branch governmental entities connecting to the state network shall remain unchanged until January 1, 2020, and shall not exceed the per employee network connection rates paid by the executive branch connecting to the state network.

(3) The house government, technology and security committee shall assess the adequacy of the basic cybersecurity rate beginning in 2022, and every two years thereafter. It shall be the duty of each entity to remit such moneys to the division of the budget as provided in section 13, and amendments thereto.

Sec. 13. (a) Under the supervision of the CISO, the KISO shall provide cybersecurity services for governmental entities, and shall make charges for such services pursuant to section 12, and amendments thereto. The furnishing of cybersecurity services by the KISO shall be a transaction to be settled in accordance with the provisions of K.S.A. 75-5516, and amendments thereto. All receipts for sales of services shall be deposited in the cybersecurity state fund.

(b) Except as otherwise provided by law and subject to the provisions of appropriation acts relating thereto, all fees and charges imposed by this act, provided or contracted for by the CISO, shall be deposited in the state treasury and credited to the cybersecurity state fund.

(c) The duty to collect payment imposed pursuant to this act shall commence on July 1, 2020.

(d) The basic cybersecurity service rate and the amounts required to be collected shall be due on October 1 of each year.

Sec. 14. (a) Governmental entities may pay for cybersecurity services from existing budgets, from grants or other revenues, or through a special assessment to offset costs associated with meeting cybersecurity service rates as specified in section 12, and amendments thereto.

(b) Any governmental entity's increase in fees or charges related to this act shall be used only for cybersecurity and no other purpose.

(c) Service or transactions with an applied cybersecurity cost recovery fee may indicate

the portion of the fee dedicated to cybersecurity on all receipts and transaction records.

Sec. 15. (a) Any entity or agency of the legislative or the judicial branch that is connecting to state network resources shall annually certify to the CISO that the entity or agency, in the opinion of such entity or agency, is maintaining substantial compliance with the national institute or standards technology cybersecurity framework or equivalent industry standard.

Sec. 16. This act shall take effect and be in force from and after its publication in the statute book.